

# Method and apparatus for protecting copyright of digital recording medium and copyright protected digital recording medium

Publication number: TW408290 (B)

Publication date: 2000-10-11

Inventor(s): KIM BYUNG-JUN [KR] +

Applicant(s): SAMSUNG ELECTRONICS CO. LTD [KR] +

Classification:

- international: G11B20/00; G11B20/10; H04N7/167; G11B20/00; G11B20/10; H04N7/167; (IPC1-7): G09C1/00

- European: G11B20/00P; H04N7/167D

Application number: TW19980121814 19981229

Priority number(s): KR19970077004 19971229

Also published as:

US6694023 (B1)

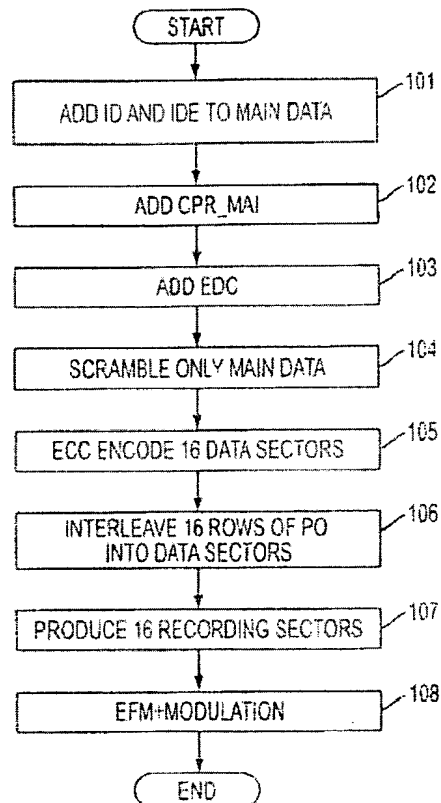
KR100403270 (B1)

CN1226064 (A)

CN1125458 (C)

## Abstract of TW 408290 (B)

A digital recording medium for protecting a copyright includes a data recording region on at least a part of which information encrypted using a cryptosystem is recorded, and a copy disapproval region on which a cypher key for decryption of the encrypted information recorded on the data recording region is recorded. When the digital recording medium is copied illegally, table identification information recorded thereon will be damaged. Thus, the information recorded on a recording medium obtained by illegally copying the digital recording medium cannot be reproduced normally. A playback apparatus for the digital recording medium includes a memory for storing the cryptosystem, a reader for reading data recorded on the digital recording medium, and a decrypter for decrypting the encrypted information recorded on the digital recording medium, based on the cypher key read from the digital recording medium by the reader.



Data supplied from the *espacenet* database — Worldwide

408200

|      |            |    |          |     |
|------|------------|----|----------|-----|
| 申請日期 | 77. 12. 29 | 案號 | 871-1814 | 公告本 |
| 類別   | G09C 1/00  |    |          |     |

(以上各欄由本局填註)

## 發明專利說明書

|        |            |  |
|--------|------------|--|
| 一、發明名稱 | 中文         | 用以保護數位化記錄媒體著作權之方法與裝置以及受著作權保護之數位化記錄媒體   |
|        | 英文         | METHOD AND APPARATUS FOR PROTECTING COPYRIGHT OF DIGITAL RECORDING MEDIUM AND COPYRIGHT PROTECTED DIGITAL RECORDING MEDIUM<br>408200 |
| 二、發明人  | 姓名(中文)     | 1. 金秉俊   |
|        | 姓名(英文)     | 1. KIM, Byung Jun  |
|        | 國籍         | 1. 南韓  |
|        | 住、居所       | 1. 大韓民國京畿道水原市八達區梅灘2洞198-81號  |
| 三、申請人  | 姓名(名稱)(中文) | 1. 三星電子股份有限公司  |
|        | 姓名(名稱)(英文) | 1. Samsung Electronics Co., Ltd.   |
|        | 國籍         | 1. 南韓  |
|        | 住、居所(事務所)  | 1. 大韓民國京畿道水原市八達區梅灘洞416號  |
|        | 代表人姓名(中文)  | 1. 尹鍾龍   |
|        | 代表人姓名(英文)  | 1. JONG YONG YUN   |

408290

(由本局填寫)

承辦人代碼：

A6

B6

大類：

IPC分類：

本案已向：

國(地區) 申請專利，申請日期：

案號：

，☐有 ☒無主張優先權

大韓民國

1997年12月29日

97-77004

有關微生物已寄存於：

，寄存日期：

，寄存號碼：

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

線

經濟部中央標準局員工消費合作社印製

## 四、中文發明摘要(發明之名稱：

用以保護數位化記錄媒體著作權之方法與裝置以及受著作權保護之數位化記錄媒體)

本發明係一種用以保護著作權的數位化記錄媒體，該媒體包括一資料記錄區域，其上至少有一部份係記錄使用某種密碼系統予以加密的資訊；和一禁止拷貝區域，其上係記錄對資料記錄區域所記錄之加密資訊予以解密的密碼鑰。當非法拷貝該數位化記錄媒體時，記錄於其上的表識別資訊將會損壞。因此，經由非法拷貝該數位化記錄媒體而獲得的記錄媒體於其上的記錄資訊便無法正常重製。一種數位化記錄媒體的重放裝置，該裝置包括：一記憶體，用以儲存密碼系統；一讀取器，用以讀取數位化記錄媒體上所記錄的資料；和一解密器，可根據讀取器從數位化記錄媒體所讀取的密碼鑰而對數位化記錄媒體上所記錄的加密資訊予以解密。

## 英文發明摘要(發明之名稱：

METHOD AND APPARATUS FOR PROTECTING COPYRIGHT OF DIGITAL RECORDING MEDIUM AND COPYRIGHT PROTECTED DIGITAL RECORDING MEDIUM

A digital recording medium for protecting a copyright includes a data recording region on at least a part of which information encrypted using a cryptosystem is recorded, and a copy disapproval region on which a cypher key for decryption of the encrypted information recorded on the data recording region is recorded. When the digital recording medium is copied illegally, table identification information recorded thereon will be damaged. Thus, the information recorded on a recording medium obtained by illegally copying the digital recording medium cannot be reproduced normally. A playback apparatus for the digital recording medium includes a memory for storing the cryptosystem, a reader for reading data recorded on the digital recording medium, and a decrypter for decrypting the encrypted information recorded on the digital recording medium, based on the cypher key read from the digital recording medium by the reader.

## 五、發明說明(1)

### 發明背景

#### 1. 發明領域

本發明係有關一種數位化記錄媒體的著作權保護，尤指一種儲存加密資料之數位化記錄媒體的著作權保護方法和裝置以及一種受著作權保護的數位化記錄媒體。

#### 2. 相關技藝說明

不論未來和目前，用於影音(A/V)設備或電腦相關設備的所有內容或軟體，必然會受到著作權的保護。因此，現正依照種種標準或規則來開發具有種種著作權保護功能的硬體或軟體。

目前已開發出或計劃提出的著作權保護技術之一係採用密碼系統的原理。現有以「資料加密標準(DES)」作為代表的對稱式密碼系統以及「RSA (Riverst, Shamir & Adleman)」作為代表的非對稱式密碼系統可供當作對資訊或信息本身予以加密的密碼系統。可用來實現前述之密碼系統的方法有一種認證系統和一種內容編密系統(CSS)。可供當作認證系統的則有使用者認證、數位簽名或信息認證。

Macrovision是一種廣泛被採用的著作權保護技術，可防止數位轉類比的拷貝。例如，若企圖拷貝或複製到習用錄放影機(VCR)的類比式磁帶上，Macrovision就會使同步訊號連續不斷地隨機變更，以致急驟降低畫質。屬於另一種著作權保護技術的「內容編密系統(CSS)」則同時運用認證系統與密碼系統，以防止數位對數位的拷貝。CSS

## 五、發明說明(2)

係用以保護安裝在一電腦上的DVD(數位化多用途光碟片)-ROM光碟機及一DVD解密卡的著作權。等DVD-ROM光碟機與DVD解密卡彼此認證後，DVD-ROM上所記錄的加密A/V資料便可經由解密卡予以解密。也就是說，DVD-ROM光碟機係使用一內建晶片或程式來執行有關DVD解密卡的認證工作，而DVD解密卡也使用一內建晶片或程式來執行認證工作與資料解碼作業。

同時，DVD播放機則包括一獨立晶片或一微控制程式，不需執行認證程序便能對加密資料予以解密，並讀取和重製一由DVD的加密A/V資料。

使用前述的著作權保護技術，只能防止一般使用者的擅自拷貝，但卻不能防止拷貝技術專家的擅自拷貝。

### 發明簡要說明

為了解決前述各種問題，本發明的一個目的係在於提供一種儲存加密資料之數位化記錄媒體的著作權保護方法。

本發明的另一目的係在於提供一種受著作權保護的數位化記錄媒體。

本發明的再一目的係在於提供一種使用受著作權保護之數位化記錄媒體的裝置。

為了達成前述之目的，本發明係提供一種用以保護有關數位化記錄媒體之著作權的著作權保護方法，該著作權保護方法包括下列各步驟：(a)使用一種密碼系統對待記錄的資訊予以加密；(b)將步驟(a)所加密的資訊記錄到數

(請先閱讀背面之注意事項再填寫本頁)

訂

線

## 五、發明說明(3)

位化記錄媒體上；和(c)利用一種禁止對密碼鑰拷貝的方式，將這密碼鑰必需記錄到數位化記錄媒體上，以便對步驟(a)所加密的資訊予以解密。

本發明亦提供一種數位化記錄媒體，其包括：一資料記錄區域，其上至少有一部份係記錄使用某種密碼系統予以加密的資訊；和一禁止拷貝區域，其上係記錄對資料記錄區域所記錄之加密資訊予以解密的必要密碼鑰。

本發明另提供一種數位化記錄媒體的重放裝置，該媒體包括一資料記錄區域，其上至少有一部份係記錄使用某種密碼系統予以加密的資訊；和一禁止拷貝區域，其上係記錄對資料記錄區域所記錄之加密資訊予以解密的必要密碼鑰，該重放裝置則包括：一記憶體，用以儲存密碼系統；一讀取器，用以讀取數位化記錄媒體上所記錄的資料；和一解密器，可根據讀取器從數位化記錄媒體所讀取的密碼鑰而對數位化記錄媒體上所記錄的加密資訊予以解密。

本發明再提供一種數位化記錄和/或重製裝置，其包括：一數位化記錄媒體，該媒體包括一資料記錄區域，其上至少有一部份係記錄使用某種密碼系統予以加密的資訊；和一禁止拷貝區域，其上係記錄對資料記錄區域所記錄之加密資訊予以解密的密碼鑰；一記憶體，用以儲存密碼系統；一讀取器，用以讀取數位化記錄媒體上所記錄的資料；和一解密器，可根據讀取器從數位化記錄媒體所讀取的密碼鑰而對數位化記錄媒體上所記錄的加密資訊予

(請先閱讀背面之注意事項再填寫本頁)

訂

線

## 五、發明說明(4)

以解密。

### 圖式簡要說明

茲列舉較佳實施例並配合參閱圖式，將本發明的前述目的及其它優點詳述於後，其中：

圖1為一流程圖，係用以解釋DVD-ROM上記錄有資料時的訊號處理情形；

圖2係顯示一種BCA碼的結構；

圖3為一流程圖，係用以解釋依據本發明其中之一實施例所構成之DVD-ROM上記錄有資料時的訊號處理情形；和

圖4為一方塊圖，顯示出依據本發明另一實施例所構成的一種數位化記錄/重製裝置。

### 較佳實施例詳細說明

現請配合參閱圖式予以說明本發明的若干較佳實施例。

依據本發明的一實施例而將加密資料記錄到一數位化記錄媒體時，是把該加密資料之解密的密碼鑰記錄在相關數位化記錄媒體的禁止拷貝區域。是以，重放裝置只有在能重製數位化記錄媒體上所記錄的密碼鑰時，方可重製原被記錄在該數位化記錄媒體上，諸如節目或資訊之類的加密資料。在依據本發明所構成的若干實施例中，於使用種種密碼系統，包括對稱式密碼系統和非對稱式密碼系統將資料加密後，便將這加密資料記錄到數位化記錄媒體的資料記錄區域，另將資料加密所用的密碼鑰記錄到設於該

(請先閱讀背面之注意事項再填寫本頁)

訂

線



## 五、發明說明(5)

資料記錄區域的外側區之禁止拷貝區域。結果，資料記錄區域是由一導入(lead-in)區，一使用或資料區，和一導出(lead-out)區所組成，而禁止拷貝區域則位在資料記錄區域的外側區。尤其，數位化記錄媒體如果是一片光碟，該禁止拷貝區域即位在導入區的外側區，亦即光學頭可讀取記錄在禁止拷貝區域之資料的位置。

在說明本發明的第一實施例之前，請先配合參閱圖1說明有關DVD(數位式多用途光碟片)-ROM的一般資料記錄方法。

將諸如影音(A/V)資料或節目的軟體記錄到DVD-ROM上時，是藉由該資料或節目經分割而取得之2048位元組主資料的單位，對該資料或節目進行訊號處理。在步驟101中，是先把4位元組的識別(ID)資料和一個用於該ID的2位元組ID偵錯碼(IDE)加到各主資料內。接著在步驟102中，把一個6位元組的著作權管理資料CPR\_MAI加入其內。然後把一個適用於所有ID、IDE、CPR\_MAI及主資料的偵錯碼(EDC)加入其內(步驟103)。等加入EDC後，只將主資料編密(步驟104)。執行完步驟101至104，即產生一個資料磁區。

對16個資料磁區執行資料磁區的錯誤校正(ECC)編碼(步驟105)。將ECC編碼所取得之16列的同位外(PO)部在資料磁區範圍內予以交錯(步驟106)。於是，產生16個記錄磁區(步驟107)。把各記錄磁區分成26個同步訊框，再用一個八轉十四正號(EFM+)表對各該同步訊框進行

(請先閱讀背面之注意事項再填寫本頁)

訂

線

## 五、發明說明(6)

EFM+調變(步驟108)。該EFM+調變是從把資料記錄到光碟片(CD)上所用的EFM調變資料修改而成，以便適合於把資料記錄到唯讀DVD光碟片(DVD-ROM)上。實際上，這EFM+調變是個八轉十六調變，可將8位元符號轉換成以二進位碼表示的16位元代碼字。執行完步驟108，即產生16個物理磁區。

步驟108所使用的EFM+表符合DVD-ROM的規格，係由一個主轉換表與一個替換表所組成。主轉換表與替換表各有四種狀態。各狀態均有分別與若干符號各自對應的16位元代碼字，以及與該等代碼字各自對應的次一狀態數值。作為參考，主轉換表中與256個符號對應的代碼字之間具有締合關係。因為各狀態都有代碼字和對應的次一狀態數值，所以數位總和差分(DSV)會與一個直流(DC)位準儘可能近似。由於DSV更近似一個直流位準，縱然在DVD-ROM發生偏心現象或光碟片表面有損傷的情況下，亦可發揮穩定訊號特性。

在本發明的這一實施例中，待記錄的資料是以前述之EFM+表經變化而成的EFM+表予以調變，從而可將加密資料記錄到一記錄媒體上。另外，在此實施例中，代表對資料加密所用之變體EFM+表的表號(table number)，也用來作為一密碼鑰，並被記錄在該記錄媒體的禁止拷貝區域，用以保護儲存該資料之相關記錄媒體的著作權。為求清晰，符合DVD-ROM規格的EFM+表定義為「基本EFM+表」，從基本EFM+表修改而成的EFM+表則定義為「變

(請先閱讀背面之注意事項再填寫本頁)

訂

線

## 五、發明說明(7)

體EFM+表」。

為使符合DVD-ROM規格的基本EFM+表在—DVD記錄和/或重製裝置中不致發生錯誤的範圍裡加以變更，本發明的此實施例是讓前述之主轉換表中之十進位數0到255的對應符號移一位。例如，當主轉換表包括一個與符號數值「0」對應的代碼字「0010 0000 0000 1001」，一個與符號數值「1」對應的代碼字「0010 0000 0001 0010」，和一個與符號數值「2」對應的代碼字「0010 0001 0010 0000」時，變體主轉換表其中之一便有一個與符號數值「0」對應的代碼字「0010 0000 0001 0010」和一個與符號數值「1」對應的代碼字「0010 0001 0010 0000」。前述基本EFM+表的變更方法，亦即使基本EFM+表中符號-代碼字關係重新締合而產生變體EFM+表的方法，對熟悉本項技藝人士為顯而易知。因此，其詳細實現方法將不予贅述。

以前述之方式變更主轉換表時，可從基本EFM+表獲得255個變體EFM+表。在此實施例中，主轉換表的符號數值係用來當作各EFM+表的表號，以供區別包括基本EFM+表在內總計256個的EFM+表。因此，具有一個與未變更主轉換表中之符號數值「1」對應的代碼字，並以其當作與本身符號數值「0」對應之代碼字的變體EFM+表，表號便是「1」。另外，具有未變更主轉換表的基本EFM+表，其表號則為「0」。該等表號可用一個位元組表示，以及可改變成任何數字，或可列入製造原廠在光碟片上所

(請先閱讀背面之注意事項再填寫本頁)

訂

線

## 五、發明說明(8)

指定的序號內。表號是將對應軟體予以解碼的要件，因此會被記錄到DVD-ROM的禁止拷貝區域。

後文將配合參閱圖2予以說明DVD-ROM的禁止拷貝區域，其中記錄依據本發明一實施例而將待記錄資訊加以調變所用變體EFM+表的對應表號。

DVD-ROM包含一個作為禁止拷貝資料記錄區域的叢發切割區(burst cutting area, BCA)。記錄在BCA之上的具有一個一系列的BCA前同步訊號欄，一個由 $4n$ (其中 $1 \leq n \leq 12$ ，而 $n$ 是一個整數)所構成的BCA資料欄，和一個一系列的后同步訊號欄，其中各列的大小為5位元組。這三個BCA欄係連續被記錄在一DVD上，中間毫無間隙。BCA前同步訊號欄具有一個1位元組的BCA同步 $SB_{BCA}$ 和位在這 $SB_{BCA}$ 之後的一個4位元組的BCA前同步訊號。BCA資料欄具有一個屬於各列引導部的BCA再同步 $RS_{BCA}$ ，若干資訊資料 $I_0, I_1, I_{16n-5}$ ，和一個偵錯碼 $ECC_{BCA}$ 。各該資訊資料及偵錯碼的大小均為4位元組。

在本發明的第一實施例中，前述之BCA的BCA前同步訊號，尤其這BCA前同步訊號的最後位元組係用來記錄表號。因此，BCA前同步訊號即變成「00h 00h 00h XXh」，其中包括代表用於調變待記錄資訊之變體EFM+表表號的「XXh」。如果以DVD-ROM規格所定義的基本EFM+表來調變資料，BCA前同步訊號就變成「00h 00h 00h 00h」。因此，本發明可與不支援變體EFM+表的DVD重放裝置相容。

(請先閱讀背面之注意事項再填寫本頁)

訂

線

## 五、發明說明(9)

圖3為一流程圖，係用以解釋本發明第一實施例所用的一種從待記錄資料產生16個物理磁區的方法。

在圖3中，步驟101至107均與所配合參閱圖1所述者相同。是以，在此不予贅述。在步驟310中，欲記錄加密資料時，便從除了基本EFM+表以外的其它255個變體EFM+表中選用一個。

該256個EFM+表是被儲存在一DVD記錄和/或重製裝置的儲存器(未顯示)裡，並從這儲存器選擇待記錄和/或重製之資料調變所用的EFM+表。該EFM+表是以一種能重新締合符號-代碼字關係而產生前述之256個EFM+表的可變EFM+表形式予以儲存在儲存器中。在此種情況下，是將一個由可變EFM+表而獲得並與待記錄和/或重製之資訊對應的變體EFM+表儲存在一獨立隨機存取記憶體(RAM)裡，並用儲存在這獨立RAM裡的變體EFM+表來調變和/或解調待記錄和/或重製的資訊。經由如此做時，就可按照意欲的速率對資料解調。或者，改將256個EFM+表儲存在一唯讀記憶體(ROM)裡。在步驟320中，是以選定的變體EFM+表來調變待記錄的資訊。於是，便產生16個物理磁區。

然而，如果所有資料包括待記錄到一DVD上的資訊均使用一變體EFM+表予以調變，然後再被記錄到一DVD上，那麼在DVD的重放期間就會發生相容性方面的問題。是以，待記錄到DVD導入區的資料係以基本EFM+表予以調變，而待記錄到DVD之資訊記錄區上的資訊則用一變體

(請先閱讀背面之注意事項再填寫本頁)

訂

線

## 五、發明說明(10)

EFM+表來調變。

在步驟330中，是將代表一個用以將資訊記錄到DVD-ROM上之變體EFM+表的獨立資料，亦即一個諸如前述之表號的密碼鑰被記錄到DVD-ROM的一個獨立區域上，亦即一個BCA前同步訊號。

當重製DVD-ROM時，DVD重放裝置會先從這DVD-ROM讀取第一個用以認可一表號的BCA碼。接著，DVD重放裝置中的一個解調器會從一個內部表RAM讀取一個與這認可表號對應的變體EFM+表，再對原記錄在這DVD-ROM上的資訊，例如A/V資料或節目加以解調。

前述之實施例可輕易應用到A/V設備或與電腦相關的設備上，且實質上並不算昂貴，其與現有所使用的需要分割硬體或軟體和採用一共同標準之設備的著作權保護技術有所不同。

本發明前述之第一實施例是以一個使用EFM+表的資料記錄調變來當作密碼系統。然而，本發明並不以前述之實施例為侷限。因此，本發明可應用到以種種密碼系統來儲存加密資料的數位化記錄媒體，以及該數位化記錄媒體所用的種種數位化記錄和/或重製系統。

圖4係顯示依據本發明第二實施例所構成的一種數位化記錄和/或重製裝置。圖4中所示的裝置係使用資料記錄調變現有的記錄調變方法，未經任何修改，同時也採用另一種密碼系統，據以對待記錄的資訊加密和/或對準備重製加密資訊予以解密。

(請先閱讀背面之注意事項再填寫本頁)

訂

線

## 五、發明說明(11)

圖4的裝置係執行與一光碟片41有關之加密資訊的記錄和/或重製工作。該裝置包括一個對光碟片41的記錄器/讀取器43，一個用以儲存密碼系統的記憶體45，和一個使用記憶體45所儲存之密碼系統以便對資訊加密或解密的加密器/解密器47。

光碟片41包括一個用以記錄加密資訊的資料記錄區域，和一個作為禁止拷貝區域的BCA。BCA上所記錄的是一個能對資料記錄區域上所記錄之加密資訊予以解密的密碼鑰。用以記錄密碼鑰的那一部份是BCA前同步訊號。然而，本發明並不受這記錄位置的限制，密碼鑰亦可記錄在BCA資料欄中未定義的部位。BCA係形成於光碟片中央孔口及一導入區域之間的一透明視窗的一部位上。尤其，BCA係形成於記錄器/讀取器43之光學頭可讀取記錄在BCA上所記錄之資料的一個位置。一DVD-ROM、一DVD-RAM(隨機存取數位式多用途光碟片)或混合DVD均可用來作為圖4之裝置所使用的光碟片41。混合DVD具有一個唯讀的ROM區和一個可重覆寫入的RAM區作為資料記錄區域。

當圖4之裝置重製含有加密資訊的光碟片41時，記錄器/讀取器43會先讀取裝入托盤(未顯示)內之光碟片41的BCA上所記錄的密碼鑰，再讀取資料記錄區域所記錄的加密資訊。然後把加密資訊及密碼鑰供應給加密器/解密器47。於是該加密器/解密器47使用儲存在記憶體45裡的讀取密碼鑰及密碼系統，將加密資訊予以解密。接著將解密

(請先閱讀背面之注意事項再填寫本頁)

訂

線

## 五、發明說明(12)

資訊供應給訊號處理器(未顯示)。

光碟片41資料記錄區域上所記錄的加密資訊，可用現有的種種加密系統或技術予以加密。因此，在此種情況下，記憶體45儲存了依據若干加密技術所製成的密碼系統時，圖4的裝置便可利用記憶體45所儲存的一個對應密碼系統的機構和BCA上所記錄的一個密碼鑰訊號，對光碟片41上所儲存的資料解密，和使用種種密碼系統予以加密。此外，當記憶體45實施為一個RAM時，記憶體45所記錄的密碼系統也能改變成另一種密碼系統。

同時，光碟片41若是合法販售或提供的DVD-RAM或混合DVD，圖4的裝置可用原已記錄在BCA上的密碼鑰對新資訊加密，並將加密的新資訊記錄到光碟片41上，或者將能用BCA上所記錄之密碼鑰予以解碼的加密資訊記錄到光碟片41上。因此，在此種情況中，軟體供應商能提供僅給予合法的用戶端在光碟片41內所添加的加密資訊所包含的內容，不需另行確認該光碟片41是否為合法擁有。

前述之第二實施例業已說明一種數位化記錄媒體所用的記錄及重製裝置。然而，凡熟悉本項技藝人士顯然可易於推知，該第二實施例亦可在本發明所屬範圍內具體實現一種只能重製數位化記錄媒體的裝置。

如前所述，這種保護著作權之方法與裝置以及受著作權保護之數位化記錄媒體可供保護有關利用數位化媒體所販售或提供之內容的著作權。此外，因為可使用現行的調變表來實現著作權保護的功能，故能以低成本製造出受著作

(請先閱讀背面之注意事項再填寫本頁)

訂

線



## 五、發明說明(13)

權保護之數位化記錄媒體的重放裝置。

## 圖式元件標號說明

|     |    |         |    |
|-----|----|---------|----|
| 光碟片 | 41 | 記錄器/讀取器 | 43 |
| 記憶體 | 45 | 加密器/解密器 | 47 |

(請先閱讀背面之注意事項再填寫本頁)

訂  
線

## 六、申請專利範圍

1. 一種用以保護有關數位化記錄媒體之著作權的著作權保護方法，該著作權保護方法包括下列各步驟：
  - (a) 使用一種密碼系統對待記錄的資訊予以加密；
  - (b) 將步驟(a)所加密的資訊記錄到數位化記錄媒體上；和
  - (c) 利用一種禁止對密碼鑰拷貝的方式，將這密碼鑰記錄到數位化記錄媒體上，以便對步驟(a)所加密的資訊予以解密。
2. 如申請專利範圍第1項所述之著作權保護方法，其中所述之數位化記錄媒體是一片光碟片，而所述之密碼鑰則被記錄在一叢發切割區(burst cutting area, BCA)。
3. 如申請專利範圍第2項所述之著作權保護方法，其中所述之密碼鑰是被記錄在一BCA前同步訊號上。
4. 如申請專利範圍第2項所述之著作權保護方法，其中所述之光碟片是一種數位化多用途光碟片(DVD)，而所述之密碼系統則是一種內容編密系統。
5. 如申請專利範圍第2項所述之著作權保護方法，其中所述之光碟片是一種DVD-ROM。
6. 如申請專利範圍第2項所述之著作權保護方法，其中所述之光碟片是一種DVD-RAM。
7. 如申請專利範圍第2項所述之著作權保護方法，其中所述之光碟片是一種混合DVD，其包括一RAM區和一ROM區作為資訊儲存區。

(請先閱讀背面之注意事項再填寫本頁)

訂  
線

## 六、申請專利範圍

8. 如申請專利範圍第 1 項所述之著作權保護方法，進一步包括下列各步驟：
- (d) 對密碼系統加以儲存；
  - (e) 從數位化記錄媒體讀取密碼鑰；和
  - (f) 使用步驟(e)所讀取的密碼鑰對數位化記錄媒體所記錄的加密資訊予以解密。
9. 如申請專利範圍第 1 項所述之著作權保護方法，其中所述之密碼系統是以一種將一預定表的符號和代碼字之間關係加以變更的變體表，以供調變待記錄資訊的調變方法，而代表該變體表的表識別資訊則用來作為密碼鑰。
10. 如申請專利範圍第 9 項所述之著作權保護方法，其中當數位化記錄媒體為 DVD 時，所述之預定表即為一個八轉十四調變正數(EFM+)表。
11. 如申請專利範圍第 10 項所述之著作權保護方法，其中所述之表識別資訊是預定 EFM+表中與變體 EFM+表中資料符號數值「0」對應的一個資料符號數值。
12. 一種數位化記錄媒體，其包括：
- 一資料記錄區域，其上至少有一部份係記錄使用某種密碼系統予以加密的資訊；和
  - 一禁止拷貝區域，其上係記錄對資料記錄區域所記錄之加密資訊予以解密的密碼鑰。
13. 如申請專利範圍第 12 項所述之數位化記錄媒體，其中所述之數位化記錄媒體是一片光碟片，而所述之密

(請先閱讀背面之注意事項再填寫本頁)

訂

訂

線

## 六、申請專利範圍

碼鑰則被記錄在一叢發切割區(burst cutting area, BCA)。

14. 如申請專利範圍第 13 項所述之數位化記錄媒體，其中所述之密碼鑰是被記錄在一 BCA 前同步訊號上。
15. 如申請專利範圍第 13 項所述之數位化記錄媒體，其中所述之光碟片是一種數位化多用途光碟片(DVD)，而所述之密碼系統則是一種內容編密系統。
16. 如申請專利範圍第 13 項所述之數位化記錄媒體，其中所述之光碟片是一種 DVD-ROM。
17. 如申請專利範圍第 13 項所述之數位化記錄媒體，其中所述之光碟片是一種 DVD-RAM。
18. 如申請專利範圍第 13 項所述之數位化記錄媒體，其中所述之光碟片是一種混合 DVD，其包括一 RAM 區和一 ROM 區作為資訊儲存區。
19. 如申請專利範圍第 12 項所述之數位化記錄媒體，其中所述之密碼系統是以一種將一預定表的符號和代碼字之間關係加以變更的變體表，以供調變待記錄資訊的調變方法，而代表該變體表的表識別資訊則用來作為密碼鑰。
20. 如申請專利範圍第 19 項所述之數位化記錄媒體，其中當數位化記錄媒體為 DVD 時，所述之預定表即為一個八轉十四調變正數(EFM+)表。
21. 如申請專利範圍第 20 項所述之數位化記錄媒體，其中所述之表識別資訊是預定 EFM+表中與變體 EFM+

(請先閱讀背面之注意事項再填寫本頁)

訂

線

## 六、申請專利範圍

表中資料符號數值「0」對應的一個資料符號數值。

22. 一種數位化記錄媒體的重放裝置，該媒體包括一資料記錄區域，其上至少有一部份係記錄使用某種密碼系統予以加密的資訊；和一禁止拷貝區域，其上係記錄對資料記錄區域所記錄之加密資訊予以解密的密碼鑰，該重放裝置則包括：

一記憶體，用以儲存密碼系統；

一讀取器，用以讀取數位化記錄媒體上所記錄的資料；和

一解密器，可根據讀取器從數位化記錄媒體所讀取的密碼鑰而對數位化記錄媒體上所記錄的加密資訊予以解密。

23. 一種數位化記錄和/或重製裝置，其包括：

一數位化記錄媒體，該媒體包括一資料記錄區域，其上至少有一部份係記錄使用某種密碼系統予以加密的資訊；和一禁止拷貝區域，其上係記錄對資料記錄區域所記錄之加密資訊予以解密的密碼鑰；

一記憶體，用以儲存密碼系統；

一讀取器，用以讀取數位化記錄媒體上所記錄的資料；和

一解密器，可根據讀取器從數位化記錄媒體所讀取的密碼鑰而對數位化記錄媒體上所記錄的加密資訊予以解密。

24. 如申請專利範圍第23項所述之數位化記錄和/或重製

(請先閱讀背面之注意事項再填寫本頁)

訂

線

## 六、申請專利範圍

裝置，其中所述之數位化記錄媒體是一片光碟片，而所述之密碼鑰則被記錄在一叢發切割區 (burst cutting area, BCA)。

25. 如申請專利範圍第 24 項所述之數位化記錄和/或重製裝置，其中所述之密碼鑰是被記錄在一 BCA 前同步訊號上。
26. 如申請專利範圍第 24 項所述之數位化記錄和/或重製裝置，其中所述之光碟片是一種數位化多用途光碟片 (DVD)，而所述之密碼系統則是一種內容編密系統。
27. 如申請專利範圍第 24 項所述之數位化記錄和/或重製裝置，其中所述之光碟片是一種 DVD-ROM。
28. 如申請專利範圍第 24 項所述之數位化記錄和/或重製裝置，其中所述之光碟片是一種 DVD-RAM。
29. 如申請專利範圍第 24 項所述之數位化記錄和/或重製裝置，其中所述之光碟片是一種混合 DVD，其包括一 RAM 區和一 ROM 區作為資訊儲存區。

(請先閱讀背面之注意事項再填寫本頁)

訂

線

圖 1

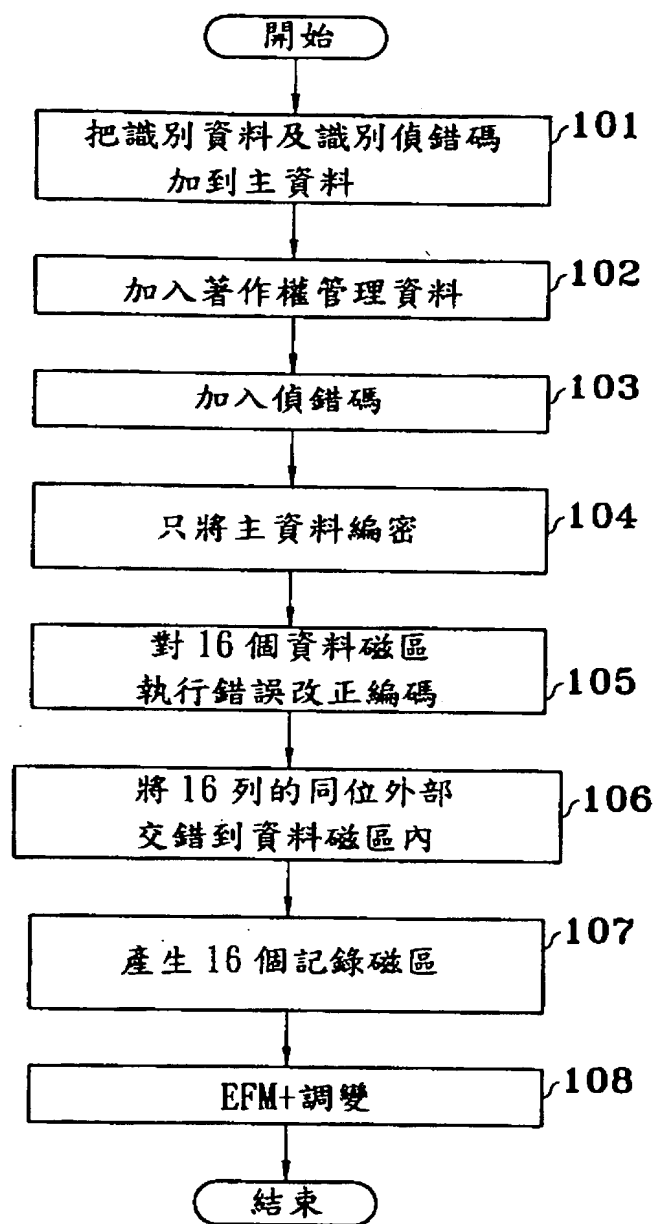


圖 2

| 5 bytes              |                              |                    |                    |                    |                  |
|----------------------|------------------------------|--------------------|--------------------|--------------------|------------------|
| 1 byte               | 4 bytes                      |                    |                    |                    |                  |
| SB <sub>BCA</sub>    | BCA-前同步訊號                    |                    |                    |                    | 1 列              |
| RS <sub>BCA1</sub>   | I <sub>0</sub>               | I <sub>1</sub>     | I <sub>2</sub>     | I <sub>3</sub>     | 4n 列<br>(1≤n≤12) |
| RS <sub>BCA1</sub>   | I <sub>4</sub>               | I <sub>5</sub>     | I <sub>6</sub>     | I <sub>7</sub>     |                  |
| RS <sub>BCA1</sub>   | ⋮                            | ⋮                  | ⋮                  | ⋮                  |                  |
| RS <sub>BCA1</sub>   | ⋮                            | ⋮                  | ⋮                  | ⋮                  |                  |
| RS <sub>BCA2</sub>   | ⋮                            | ⋮                  | ⋮                  | ⋮                  |                  |
| ⋮                    |                              |                    |                    |                    |                  |
| ⋮                    |                              |                    |                    |                    |                  |
| RS <sub>BCA1-1</sub> |                              |                    |                    |                    |                  |
| RS <sub>BCA1</sub>   |                              |                    |                    |                    |                  |
| RS <sub>BCA1</sub>   | 資訊                           |                    |                    |                    |                  |
| RS <sub>BCA1</sub>   |                              |                    |                    |                    |                  |
| RS <sub>BCA1</sub>   |                              |                    |                    |                    |                  |
| RS <sub>BCA1+1</sub> |                              |                    |                    |                    |                  |
| ⋮                    |                              |                    |                    |                    |                  |
| ⋮                    |                              |                    |                    |                    |                  |
| RS <sub>BCAn-1</sub> |                              |                    |                    |                    |                  |
| RS <sub>BCAn</sub>   | ⋮                            | ⋮                  | ⋮                  | ⋮                  |                  |
| RS <sub>BCAn</sub>   | ⋮                            | ⋮                  | ⋮                  | ⋮                  |                  |
| RS <sub>BCAn</sub>   | I <sub>16n-5</sub>           | I <sub>16n-7</sub> | I <sub>16n-5</sub> | I <sub>16n-5</sub> |                  |
| RS <sub>BCAn</sub>   | EDC <sub>BCA</sub> (4 bytes) |                    |                    |                    |                  |
| RS <sub>BCA13</sub>  | C <sub>00</sub>              | C <sub>10</sub>    | C <sub>20</sub>    | C <sub>30</sub>    | 4 列              |
| RS <sub>BCA13</sub>  | ⋮                            | ⋮                  | ⋮                  | ⋮                  |                  |
| RS <sub>BCA13</sub>  | ECC <sub>BCA</sub>           |                    |                    |                    |                  |
| RS <sub>BCA13</sub>  | C <sub>03</sub>              | C <sub>13</sub>    | C <sub>23</sub>    | C <sub>33</sub>    |                  |
| RS <sub>BCA14</sub>  | BCA-後同步訊號                    |                    |                    |                    | 1 列              |
| RS <sub>BCA15</sub>  |                              |                    |                    |                    |                  |



圖 3

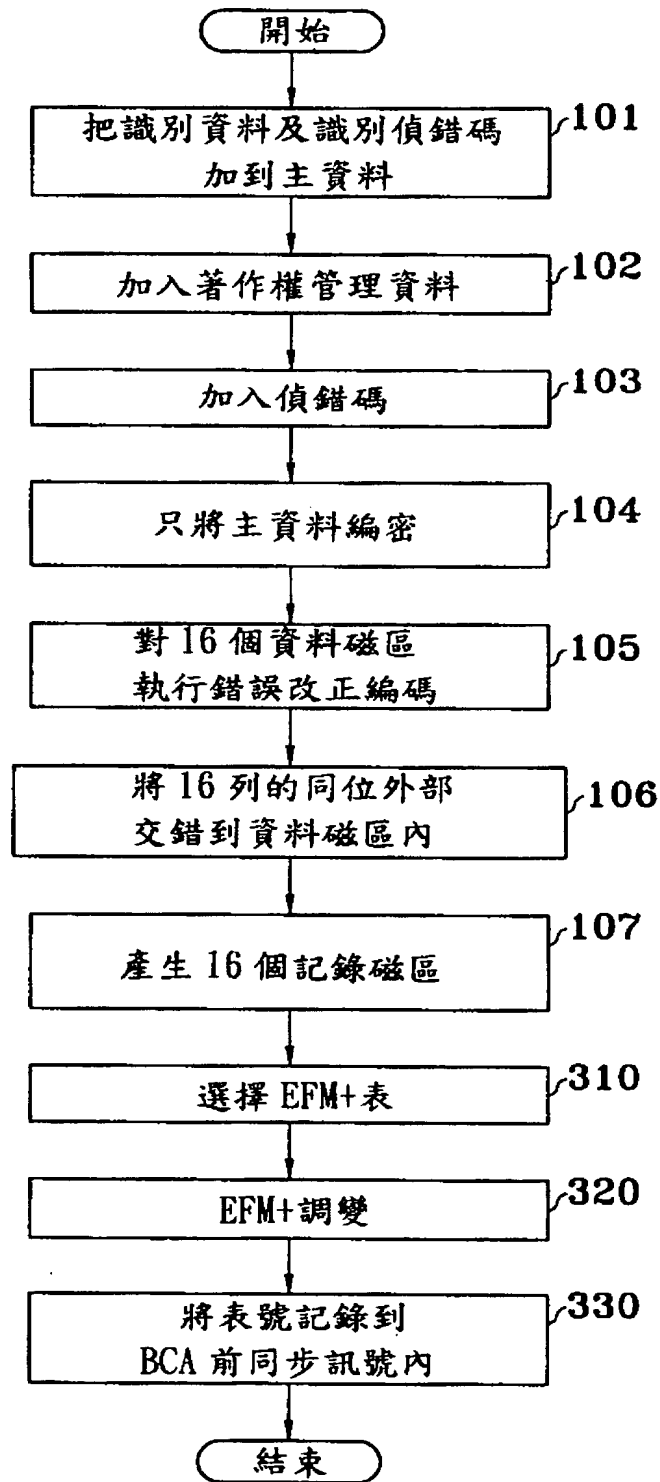
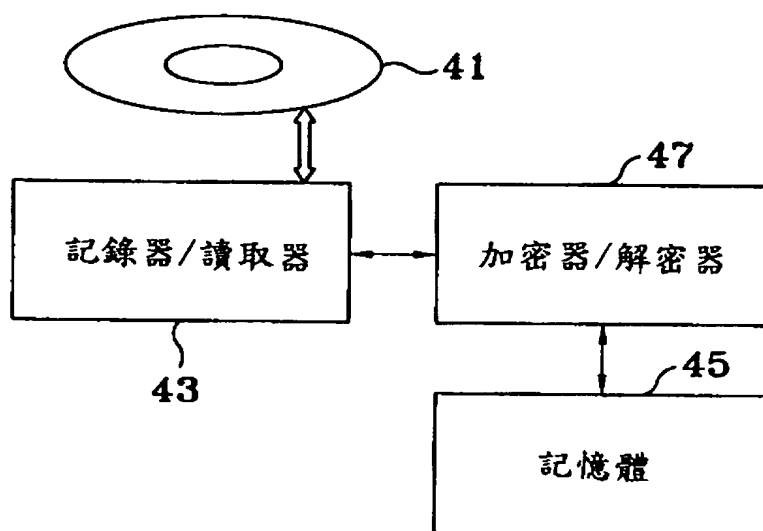


圖 4



## 中華民國專利公報 [19] [12]

[11]公告編號：408290

[44]中華民國 89年(2000) 10月11日

發明

全 5 頁

[51] Int.Cl 06: G09C1/00

[54]名稱：用以保護數位化記錄媒體著作權之方法與裝置以及受著作權保護之數位化記錄媒體

[21]申請案號：087121814

[22]申請日期：中華民國 87年(1998) 12月29日

[72]發明人：

金秉俊

韓國

[71]申請人：

三星電子股份有限公司

韓國

[74]代理人：羅炳榮 先生

1

[57]申請專利範圍：

1. 一種用以保護有關數位化記錄媒體之著作權的著作權保護方法，該著作權保護方法包括下列各步驟：
  - (a) 使用一種密碼系統對待記錄的資訊予以加密；
  - (b) 將步驟(a)所加密的資訊記錄到數位化記錄媒體上；和
  - (c) 利用一種禁止對密碼鑰拷貝的方式，將這密碼鑰記錄到數位化記錄媒體上，以便對步驟(a)所加密的資訊予以解密。
2. 如申請專利範圍第1項所述之著作權保護方法，其中所述之數位化記錄媒體是一片光碟片，而所述之密碼鑰則被記錄在一叢發切割區(burst cutting area, BCA)。
3. 如申請專利範圍第2項所述之著作權保護方法，其中所述之密碼鑰是被記錄在

2

- 一 BCA 前同步訊號上。
4. 如申請專利範圍第2項所述之著作權保護方法，其中所述之光碟片是一種數位化多用途光碟片(DVD)，而所述之密碼系統則是一種內容編密系統。
5. 如申請專利範圍第2項所述之著作權保護方法，其中所述之光碟片是一種 DVD-ROM。
10. 6. 如申請專利範圍第2項所述之著作權保護方法，其中所述之光碟片是一種 DVD-RAM。
15. 7. 如申請專利範圍第2項所述之著作權保護方法，其中所述之光碟片是一種混合 DVD，其包括一 RAM區和一 ROM區作為資訊儲存區。
8. 如申請專利範圍第1項所述之著作權保護方法，進一步包括下列各步驟：
  - (d) 對密碼系統加以儲存；

- (e)從數位化記錄媒體讀取密碼鑰；和  
(f)使用步驟(e)所讀取的密碼鑰對數位化記錄媒體所記錄的加密資訊予以解密。
- 9.如申請專利範圍第1項所述之著作權保護方法，其中所述之密碼系統是以一種將一預定表的符號和代碼字之間關係加以變更的變體表，以供調變待記錄資訊的調變方法，而代表該變體表的表識別資訊則用來作為密碼鑰。
- 10.如申請專利範圍第9項所述之著作權保護方法，其中當數位化記錄媒體為DVD時，所述之預定表即為一個八轉十四調變正數(EFM+)表。
- 11.如申請專利範圍第10項所述之著作權保護方法，其中所述之表識別資訊是預定EFM+表中與變體EFM+表中資料符號數值「0」對應的一個資料符號數值。
- 12.一種數位化記錄媒體，其包括：  
一資料記錄區域，其上至少有一部份係記錄使用某種密碼系統予以加密的資訊；和  
一禁止拷貝區域，其上係記錄對資料記錄區域所記錄之加密資訊予以解密的密碼鑰。
- 13.如申請專利範圍第12項所述之數位化記錄媒體，其中所述之數位化記錄媒體是一片光碟片，而所述之密碼鑰則被記錄在一叢發切割區(burst cutting area, BCA)。
- 14.如申請專利範圍第13項所述之數位化記錄媒體，其中所述之密碼鑰是被記錄在一BCA前同步訊號上。
- 15.如申請專利範圍第13項所述之數位化記錄媒體，其中所述之光碟片是一種數位化多用途光碟片(DVD)，而所述之密碼系統則是一種內容編密系統。
- 16.如申請專利範圍第13項所述之數位化記錄媒體，其中所述之光碟片是一

- 種DVD-ROM。
- 17.如申請專利範圍第13項所述之數位化記錄媒體，其中所述之光碟片是一種DVD-RAM。
5. 18.如申請專利範圍第13項所述之數位化記錄媒體，其中所述之光碟片是一種混合DVD，其包括一RAM區和一ROM區作為資訊儲存區。
- 19.如申請專利範圍第12項所述之數位化記錄媒體，其中所述之密碼系統是以一種將一預定表的符號和代碼字之間關係加以變更的變體表，以供調變待記錄資訊的調變方法，而代表該變體表的表識別資訊則用來作為密碼鑰。
10. 20.如申請專利範圍第19項所述之數位化記錄媒體，其中當數位化記錄媒體為DVD時，所述之預定表即為一個八轉十四調變正數(EFM+)表。
15. 21.如申請專利範圍第20項所述之數位化記錄媒體，其中所述之表識別資訊是預定EFM+表中與變體EFM+表中資料符號數值「0」對應的一個資料符號數值。
20. 22.一種數位化記錄媒體的重放裝置，該媒體包括一資料記錄區域，其上至少有一部份係記錄使用某種密碼系統予以加密的資訊；和一禁止拷貝區域，其上係記錄對資料記錄區域所記錄之加密資訊予以解密的密碼鑰，該重放裝置則包括：  
一記憶體，用以儲存密碼系統；  
一讀取器，用以讀取數位化記錄媒體上所記錄的資料；和  
一解密器，可根據讀取器從數位化記錄媒體所讀取的密碼鑰而對數位化記錄媒體上所記錄的加密資訊予以解密。
25. 30. 23.一種數位化記錄和／或重製裝置，其包括：  
一數位化記錄媒體，該媒體包括一資料記錄區域，其上至少有一部份係記錄使
35. 40.

用某種密碼系統予以加密的資訊；和一禁止拷貝區域，其上係記錄對資料記錄區域所記錄之加密資訊予以解密的密碼鑰；

一記憶體，用以儲存密碼系統；

一讀取器，用以讀取數位化記錄媒體上所記錄的資料；和

一解密器，可根據讀取器從數位化記錄媒體所讀取的密碼鑰而對數位化記錄媒體上所記錄的加密資訊予以解密。

24.如申請專利範圍第 23 項所述之數位化記錄和／或重製裝置，其中所述之數位化記錄媒體是一片光碟片，而所述之密碼鑰則被記錄在一叢發切割區 (burst cutting area, BCA)。

25.如申請專利範圍第 24 項所述之數位化記錄和／或重製裝置，其中所述之密碼鑰是被記錄在一 BCA 前同步訊號上。

26.如申請專利範圍第 24 項所述之數位化記錄和／或重製裝置，其中所述之光碟片是一種數位化多用途光碟片 (DVD)，而所述之密碼系統則是一種內容編密系統。

27.如申請專利範圍第 24 項所述之數位化記錄和／或重製裝置，其中所述之光碟片是一種 DVD-ROM。

28.如申請專利範圍第 24 項所述之數位化記錄和／或重製裝置，其中所述之光碟片是一種 DVD-RAM。

29.如申請專利範圍第 24 項所述之數位化記錄和／或重製裝置，其中所述之光碟片是一種混合 DVD，其包括一 RAM 區和一 ROM 區作為資訊儲存區。

圖式簡單說明：

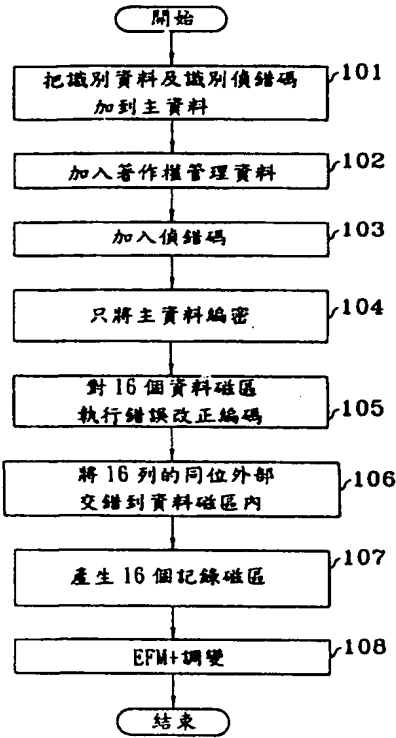
第一圖為一流程圖，係用以解釋 DVD-ROM 上記錄有資料時的訊號處理情形；

15. 第二圖係顯示一種 BCA 碼的結構；

第三圖為一流程圖，係用以解釋依據本發明其中之一實施例所構成之 DVD-ROM 上記錄有資料時的訊號處理情形；和

20. 第四圖為一方塊圖，顯示出依據本發明另一實施例所構成的一種數位化記錄／重製裝置。

(4)

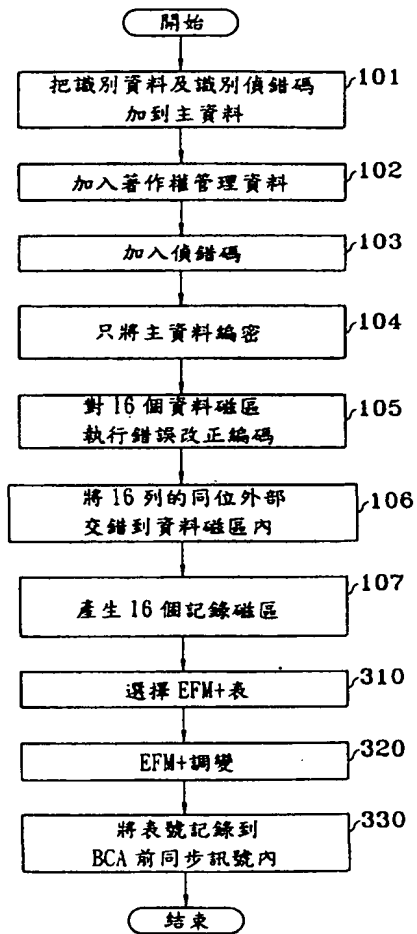


第一圖

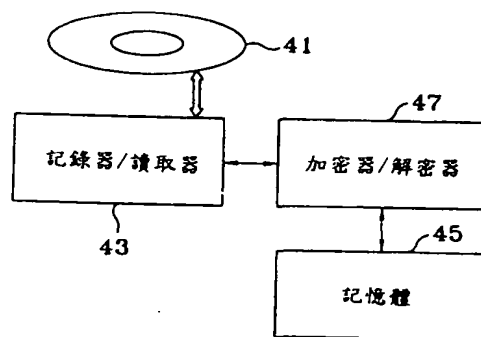
| 5 bytes              |                              |                    |                    |                    |                  |
|----------------------|------------------------------|--------------------|--------------------|--------------------|------------------|
| 1 byte               | 4 bytes                      |                    |                    |                    |                  |
| SB <sub>BCA</sub>    | BCA-前同步訊號                    |                    |                    |                    | 1 列              |
| RS <sub>BCA1</sub>   | l <sub>0</sub>               | l <sub>1</sub>     | l <sub>2</sub>     | l <sub>3</sub>     | 4n 列<br>(1≤n≤12) |
| RS <sub>BCA1</sub>   | l <sub>4</sub>               | l <sub>5</sub>     | l <sub>6</sub>     | l <sub>7</sub>     |                  |
| RS <sub>BCA1</sub>   | :                            | :                  | :                  | :                  |                  |
| RS <sub>BCA1</sub>   | :                            | :                  | :                  | :                  |                  |
| RS <sub>BCA2</sub>   | :                            | :                  | :                  | :                  |                  |
| :                    |                              |                    |                    |                    |                  |
| :                    |                              |                    |                    |                    |                  |
| RS <sub>BCA1-1</sub> |                              |                    |                    |                    |                  |
| RS <sub>BCA1</sub>   |                              |                    |                    |                    |                  |
| RS <sub>BCA1</sub>   |                              |                    |                    |                    |                  |
| RS <sub>BCA1</sub>   |                              |                    |                    |                    |                  |
| RS <sub>BCA1</sub>   |                              |                    |                    |                    |                  |
| RS <sub>BCA1+1</sub> |                              |                    |                    |                    |                  |
| :                    |                              |                    |                    |                    |                  |
| :                    |                              |                    |                    |                    |                  |
| RS <sub>BCAn-1</sub> |                              |                    |                    |                    |                  |
| RS <sub>BCAn</sub>   | :                            | :                  | :                  | :                  |                  |
| RS <sub>BCAn</sub>   | :                            | :                  | :                  | :                  |                  |
| RS <sub>BCAn</sub>   | l <sub>16n-5</sub>           | l <sub>16n-7</sub> | l <sub>16n-5</sub> | l <sub>16n-5</sub> |                  |
| RS <sub>BCAn</sub>   | EDC <sub>BCA</sub> (4 bytes) |                    |                    |                    |                  |
| RS <sub>BCA13</sub>  | C <sub>00</sub>              | C <sub>10</sub>    | C <sub>20</sub>    | C <sub>30</sub>    | 4 列              |
| RS <sub>BCA13</sub>  | :                            | :                  | :                  | :                  |                  |
| RS <sub>BCA13</sub>  | ECC <sub>BCA</sub>           |                    |                    |                    |                  |
| RS <sub>BCA13</sub>  | C <sub>03</sub>              | C <sub>13</sub>    | C <sub>23</sub>    | C <sub>33</sub>    |                  |
| RS <sub>BCA14</sub>  | BCA-後同步訊號                    |                    |                    |                    | 1 列              |
| RS <sub>BCA15</sub>  |                              |                    |                    |                    |                  |

第二圖

(5)



第三圖



第四圖